1. Roth, G., Schreiber, S.J., Pushed beyond the brink: Allee effects, environmental stochasticity, and extinction, Journal of biological dynamics 8 (1), 187-205, 2014.
2. Bashkirtseva, I., Ryashko, L., Tsvetkov, I., Sensitivity analysis of stochastic equilibria and cycles for the discrete dynamic systems, Dynamics of Continuous, Discrete and Impulsive Systems, Series A: Mathematical Analysis, 17: 501–515, 2010.

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

Куприянов А.О.*, Бабенко А.А.

Волгоградский государственный университет, г. Волгоград, Россия

*E-mail: ao.kupriyanov@yandex.ru

THE INFORMATION SECURITY RISK ASSESSMENT OF COMMERCIAL ORGANIZATIONS

Kupriyanov A.O.*, Babenko A.A.

Volgograd State University, Volgograd, Russia

In the presented method of risk assessment of information security of commercial organizations risk is expressed in the expected monetary losses for a some period. Quantitative risk assessment, expressed in monetary losses, is translated into a qualitative indicator of the overall level of risk and the information security level of the organization, which provides the management of the organization with a understandable result of the procedure.

Обширный спектр угроз информации требует комплекс мер её защиты. Процедура выбора мер защиты активов сложна и подразумевает проведение оценки рисков.

Расчёт возможного риска по всем активам организации позволяет определить уровень информационной безопасности (УИБ) организации. УИБ –показатель актуальной ситуации информационной безопасности в организации, введённый в целях информативного представления результатов оценки риска руководству организации, отражает степень защищённости организации, корректность её политики информационной безопасности, эффективность внедрённых контрмер и т.д.

Этапы процедуры оценки рисков информационной безопасности коммерческих организаций основываются на [1]:

1. Идентификация активов – определение и описание активов;
2. Оценка рисков – определение уязвимостей активов и угроз, использующих уязвимости, последствия их реализации и их описание. Оценка общего риска – суммарные ожидаемые денежные потери ИС коммерческих организаций за год;
3. Установление значения общего уровня риска и УИБ;

4. Обработка рисков – определение и описание контрмер для угроз ИБ. Установление значения общего уровня риска и УИБ с учётом заданных контрмер;
5. Подготовка результатов процедуры оценки рисков.

В представленной методике оценки рисков информационной безопасности коммерческих организаций риск выражается в ожидаемых денежных потерях за некоторый период. При этом количественная оценка рисков, выраженная в денежных потерях, переводится в наглядный качественный показатель общего уровня риска и УИБ организации, что предоставляет руководству организации наглядный и понятный результат проделанной процедуры.

1. ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство. (2018)

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ОЦЕНКИ ВНУТРЕННИХ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Куприянов А.О.*, Курина А.Д., Бабенко А.А.

Волгоградский государственный университет, г. Волгоград, Россия

*E-mail: nastyakurina@mail.ru

DEVELOPMENT OF SOFTWARE COMPLEX FOR ASSESSMENT INTERNAL THREATS TO THE SECURITY OF CONFIDENTIAL INFORMATION

Kupriyanov A.O.*, Kurina A.D., Babenko A.A.

Volgograd State University, Volgograd, Russia

Annotation. The model of assessment internal threats to security of confidential information is presented in article. As a result,software complex is developed, the optimization task of determining the most likely for the implementation of the security threat of confidential information are formulated.

Угрозы и уязвимости образуют основу риска. Прежде чем оценить риски и принять меры по их устранению необходимо определить и оценить угрозы. По статистическим данным за последние полгода количество утечек от внутреннего нарушителя почти в 1,5 раза больше чем от внешних воздействий. Особенно стоит отметить утечку конфиденциальной информации (КИ), к которой относятся персональные данные (65,8%), платежная информация (26,8%), коммерческая тайна (3,4%) [1].

Процедура анализа угроз безопасности КИ представлена в [2]. Методы, используемые для оценки угроз – количественные и качественные. Для оценки угроз выбраны два метода – методика ФСТЭК и метод экспертных оценок.